FOTREZ

CYBERWARE TESTING AND COMPLETE DATA ANALYSIS REPORT

Operating System Kali Linux

Tool used hping3

Hping3 is a tool that allows users to send custom TCP/IP packets and analyse network traffic.

Hping3 data can be used to test network performance, perform port scanning, and fingerprint remote operating systems.

ATTACK PERFORMED ON DOCKER CONTAINER

We use 3 different work space

Bot – Fotrez bot for ddos detection

Attacker – Hping3 tool

Victim – Virtual bot server

Connected to the save network configuration and workspace virtual space environment

FOTREZ

TESTING AND ANALYSIS OF DATA

Hping3 to specify a target IP address

```
-$ sudo hping3 192.168.249.128

HPING 192.168.249.128 (eth0 192.168.249.128): NO FLAGS are set, 40 headers + 0 data bytes

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=0 flags =RA seq=0 win=0 rtt 3.1 ms len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=0 flags =RA seq=1 win=0 rtt=4.2 ms

53:32 e 64 or Maa Bains flags

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=0 flags =RA seq=2 win=0 rtt=7.4 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=0 flags =RA seq=3 win=0 rtt=11.4 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=0 flags
```

ICMP mode –

```
sudo hping3 --icmp 192.168.249.128

HPING 192.168.249.128 (eth0 192.168.249.128): icmp mod e set, 28 headers + 0 data bytes

len=46 ip=192.168.249.128 ttl=64 id=64494 icmp_seq=0 r tt=10.9 ms

len=46 ip=192.168.249.128 ttl=64 id=64495 icmp_seq=1 r tt=7.0 ms

len=46 ip=192.168.249.128 ttl=64 id=64496 icmp_seq=2 r tt=4.0 ms

len=46 ip=192.168.249.128 ttl=64 id=64497 icmp_seq= tt=3.0 ms

len=46 ip=192.168.249.128 ttl=64 id=64498 icmp_seq=4 r
```

Scan Mode –

```
$ sudo hping3 --scan 1-143 192.168.249.128

Scanning 192.168.249.128 (192.168.249.128), port 1-143 143 ports to scan, use -V to see all the replies

Iport serv name | flags lttl| id | win | len |

All replies received. Done.

Not responding ports: (21 ftp) (22 ssh) (23 telnet) (2

5 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbio s-ssn)
```

Detailed output (-V)

```
sudo hping3 --scan 1-143 192.168.249.128 -V using eth0, addr: 192.168.249.175, MTU: 1500

Scanning 192.168.249.128 (192.168.249.128), port 1-143 143 ports to scan, use -V to see all the replies
```

```
Iport serv name flags Ittll id | win | len | 1 tcpmux 2 nbp

:..R.A... 64

0 0

46 3:.. R.A...

64 0 46 4 echo ..R.A... 64  0 0
```

Number of packets to send (-c)

```
sudo hping3 192.168.249.128 -p 80 -c 1

HPING 192.168.249.128 (eth0 192.168.249.128): NO FLAGS are set, 40 headers + 0 data bytes

192.168.249.128 hping statistic 1 packets transfer , 1 packets received 100%

Packet loss 000

round-trip min/avg/max = 0.3/0.1/0.2 ms

-$ sudo hping3 192.168.249.128 -p 80 -c 5

HPING 192.168.249.128 (eth0 192.168.249.128): NO FLAGS are set, 40 headers + data bytes

— 192.168.249.128 hping statistic —

5 packets transmitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms
```

send a SYN request to port 80 of our target system and see the reply

```
-$ sudo hping3 -S 192.168.249.128 -p 80 -c 3

HPING 192.168.249.128 (eth0 192.168.249.128): S set, 40 headers

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=0 win=5840 rtt=3.4 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=1 win=5840 rtt=3.8 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=2 win=5840 rtt=3.8 ms
```

Reacts to ACK scan

```
sudo hping3 -A 192.168.249.128 -p 80 -c 3

HPING 192.168.249.128 (eth0 192.168.249.128): A set, 4

0 headers + 0 data bytesHackercool Magazine'

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=R seq=0 win=0 rtt=3.7 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=R seq=1 win=0 rtt=8.0 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=R seq=2 win=0 rtt=7.2 ms
```

Denial of Service (DDoS) attack

hping3 will send 10 packets for second to the target. For example let’s send SYN packets to target port 80

```
-$ sudo hping3 --fast -S 192.168.249.128 -p 80

HPING 192.168.249.128 (eth0 192.168.249.128): S set, 4

0 headers + 0 data bytes lackercool Magazine len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA
seq=0 win=5840 rtt=7.3 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=1 win=5840 rtt=7.7 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=2 win=5840 rtt=8.2 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag s=SA seq=3 win=5840 rtt=11.6 ms

len=46 ip=192.168.249.128 ttl=64 DF id=0 sport=80 flag
```

Conclusion

With the help of current module version 0.0.0.1

We can detect an incoming ddos attack and alert the user